

JUDGE FAILLA

20 CV 00209

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X
SFM REALTY CORP.,
:

Plaintiff,
:

v. :
:

PATRICIA M. LEMANSKI,
:

Defendant.
: X

Case No.:

**MEMORANDUM OF LAW IN SUPPORT OF
PLAINTIFF'S MOTION FOR EMERGENCY INJUNCTIVE RELIEF**

FREEBORN & PETERS, LLP

Marc B. Zimmerman

Kathryn T. Lundy

230 Park Avenue, Suite 630

New York, NY 10169

(212) 218-8760

Attorneys for Plaintiff

TABLE OF CONTENTS

PRELIMINARY STATEMENT1

STATEMENT OF FACTS2

 Strict confidentiality of its methods and procedures concerning the operation
 of its business is critical to SFM’s real estate investment, development and
 management5

 SFM is vigilant in securing and protecting its confidential and trade secret
 information7

ARGUMENT10

 SFM IS ENTITLED TO INJUNCTIVE RELIEF10

 A. Standard of Review10

 B. Injunctive Relief is Warranted Under the Defense Trade Secrets Act11

 C. SFM Will Suffer irreparable Harm if this Court Does Not Grant Injunctive Relief12

 D. SFM is Likely to Succeed on the Merits of Its Underlying Claim.....16

 1. The DTSA Claim16

 2. New York’s Trade Secret Law17

 3. Breach of Contract18

 4. Breach of Duty of Loyalty18

 E. The Balance of the Equities, the Evidence, and the Public Interest Tip
 Strongly in Favor of SFM.....19

CONCLUSION.....20

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Ashland Mgmt. Inc. v. Janittn.</i> 82 N.Y.2d 395 (1993).....	18
<i>AUA Private Equity Partners. LLC v. Solo,</i> No. 17 Civ 803 (S.D.N.Y. November 6, 2017)	11
<i>AUA Private Equity Partners, LLC v. Solo,</i> No. 17-8035, 2018 WL 2684339 (S.D.N.Y. April 5, 2018).....	16
<i>Broker Genius, Inc. v. Zalta,</i> 280 F. Supp. 3d 495, 509 (S.D.N.Y. 2017)	16
<i>Citigroup Glob. Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.,</i> 598 F.3d 30 (2d Cir. 2010)	10
<i>Corp. v. Liberty Mut. Ins. Co.,</i> 152 F.3d 162 (2d Cir. 1998)	18
<i>Design Strategies. Inc. v. Davis,</i> 384 F.Supp.2d 649 (S.D.N.Y. 2005)	19
<i>Eastern Bus. Sys., Inc. v. Specialty Bus. Solutions,</i> 292 A.D.2d 336 (2d Dept. 2002)	17
<i>Estee Lauder Cos. V. Batra,</i> 430 F. Supp. 2d 158 (S.D.N.Y. 2006)	12, 13, 14
<i>Faiveley Transp. Mahmo AB v. Wabtec Corp.,</i> 559 F.3d 110 (2d Cir. 2009)	12
<i>FMC Corp. v. Taiwain Tainan Giant Indus. Co., Ltd.,</i> 730 F.2d 61 (2d Cir. 1984)	12
<i>Free Country Ltd v. Drennen,</i> 235 F.Supp.3d 559, 565 (S.D.N.Y. 2016)	16
<i>Henry Schein, Inc. v. Coak.</i> 191 F.Supp.3d 1072 (N.D. Cal. 2016).....	11
<i>Juergensen Def. Corp, v. Carleton Techs. Inc.,</i> No. 08-CV- 959A, 2010 WL 2671339 (W.D.N.Y. June 21, 2010).....	20

<i>Mickey's Linen v. Fischer</i> , No. 17 C 2154, 2017 WL 3970593 (N.D. III. September 8, 2017)	11
<i>Mission Capital Advisors LLC v. Romaka</i> , No. 15 Civ 5878, 2016 WL 11517040 (S.D.N.Y. July 22, 2016)	11
<i>N. All. Instruments, Inc. v. Haber</i> , 188 F.	18
<i>North Atlantic Instruments, Inc. v. Haber</i> , 188 F.3d 38	12, 13
<i>Payment All. Int'l, Inc. v. Ferreira</i> , 530 Supp. 2d 477	12
<i>Phansalkar v. Andersen Weinroth & Co. L.P.</i> , 344 F.3d 184 (2d Cir. 2003)	18, 19
<i>Roll-Krafi v. Grimes</i> . 177 F.Supp.2d 859 (N.D. III. 2001)	17
<i>W. Elec. Co. v. Brenner</i> , 41 N.Y.2d 291, 392 N.Y.S.2d 409, 360 N.E.2d 1091 (1977).....	19
<i>Winter v. Nat. Hus. Def Council, Inc.</i> , 555 U.S. 7 (2008).....	10

STATUTES

18 U.S.C. § 1831.....	16
18 U.S.C.A. § 1836.....	2
18 U.S.C. § 1836(3)(A)(I)	11
18 USC § 1839.....	14
18 U.S.C. § 1839(5).....	16
18 U.S.C. § 1839(6)(A)-(B).....	16
18 USC § 1839(3).....	14

Plaintiff SFM Realty Corp. ("SFM") respectfully submits this memorandum in support of its application for an *ex parte* Temporary Restraining Order ("TRO") and Preliminary Injunction against Defendant Patricia Lemanski ("Defendant").

PRELIMINARY STATEMENT

SFM seeks the Court's urgent intervention to immediately enjoin Defendant's unauthorized use of SFM's trade secrets and proprietary and confidential information to limit further serious and irreparable harm to SFM.

During a security review on or about January 3, 2020, SFM was horrified to learn that Defendant has been systemically, and without SFM's authorization, sending SFM's proprietary and confidential trade secret information beyond SFM's firewall to Defendant's personal e-mail account. Such misappropriated information included documents containing SFM's key business contact information, operating agreements, leases, vendor agreements (including fees and scope of services), technical data, methods and procedures of business operations and financial data (including loan agreements), all of which would cause irreparable harm to SFM and its business interests if divulged to a third-party or used in connection with activities competitive or harmful to SFM's business.

Notably, as an employee of SFM, Defendant was able to access her SFM emails around the clock via Microsoft Outlook and Webmail from her cell phone, mobile devices in Defendant's possession and control, Defendant's desktop computer and laptop. As such, and as outlined in detail below, there is/was no legitimate business reason for her to send SFM's proprietary and confidential trade secret information to her own personal e-mail account. The timing and circumstances of Defendant's actions demonstrate, without a doubt, they were deliberate and intended to misappropriate and convert SFM's information for her own use or

purposes, or for the benefit of a third party. Indeed, the information Defendant converted was not just information concerning matters she was working on, but also matters she played no part in and concerning SFM deals that had already closed. As set forth in detail below, SHM's preliminary search has confirmed Defendant's surreptitious actions were intentional and for no legitimate business purpose as: (1) she forwarded the same documents to herself on at least two occasions on the same day (to ensure receipt on her personal e-mail account); and (2) she contacted one of the organization's hospitality assets, a luxury hotel, directly, and without the authorization of SHM management, to obtain a comprehensive set of key confidential and trade secret information concerning hotel operation, of which she had no role in and no legitimate business interest in obtaining.

As the purloined trade secret and confidential and proprietary materials remain on Defendant's personal e-mail account (tri714@gmail.com), which is in Defendant's possession and under control, SFM seeks an emergency court order directing Defendant to return to it all misappropriated trade secret and confidential and proprietary information, certify and allow verification that she has done so, and further certify that she (via a third party computer forensic vendor retained by SFM) has destroyed all copies of any misappropriated materials.¹

STATEMENT OF FACTS

The facts relevant to the application, explained more fully in the accompanying Affidavit of Lonica Smith, dated January 9, 2020 ("Smith Aff."), are as follows:

SFM is part of The Sapir Organization, a multidisciplinary real estate investor, operator and developer whose portfolio spans multiple property classes, including commercial, residential

¹ SFM reserves the right to file a subsequent application for an order of seizure of the misappropriated materials pursuant to the Defense of Trade Secrets Act ("DTSA"), 18 U.S.C.A. § 1836, *et seq.*

and hospitality assets such as the NoMo SoHo Hotel, development properties in Miami and office buildings in Manhattan. *See* Smith Aff. at ¶ 2. Included with The Sapir Organization is Sapir Corp., Ltd., which is publicly traded on the Tel Aviv Stock Exchange. *Id.* Defendant is employed by SFM as an assistant and paralegal and is responsible for, among other things, supporting real estate transactions and closings for The Sapir Organization. *Id.* at ¶ 3. Defendant has been employed by SFM in this role since her hire on September 7, 2011.

As set forth in detail below, SFM has recently discovered that Defendant has misappropriated, converted and/or stolen SFM's proprietary information, specifically including documents and electronic data, the vast majority of which contain confidential and trade secret material. *Id.* at ¶ 4. In addition, much of this information also constitutes "inside information" under Israeli securities laws. *Id.* Based upon her misconduct and breach of SFM policy, contract and the law, SFM intends to terminate Defendant's employment. *Id.*

Specifically, during a recent security review, SFM determined that Defendant has been systemically, and without authorization, sending SFM's confidential trade secret information beyond the SFM firewall to Defendant's personal e-mail account (tri714@gmail.com). *Id.* at ¶ 5. Such misappropriated information included documents containing SFM's key business contact information, operating agreements, leases, vendor agreements (including fees and scope of services), technical data, methods and procedures of business operations and financial data (including loan agreements), all of which would cause irreparable harm to SFM and its business interests if divulged to a competitor or used in connection with activities competitive to SFM's business. *Id.*

SFM has made copies of the e-mails and attachments it has identified to date containing SFM's information misappropriated by Defendant and sent by Defendant from a SFM e-mail

account to Defendant's personal e-mail account. *Id.* at ¶ 6, Exhibit A. The timing and circumstances of Defendant's actions demonstrate they were deliberate and intended to misappropriate SFM's information. *Id.* at ¶ 7. For example, on January 3, 2020 at 11:27 a.m., Defendant sent an e-mail and attachment to her personal e-mail account containing confidential and sensitive loan modification documents. *Id.* Later that same day, at 12:58 p.m., Defendant again sent an e-mail and attachment to her personal e-mail account containing these confidential and sensitive loan modification documents. *Id.* These attachments had recently been finally executed and Defendant had no part in their drafting; there is no possible legitimate reason Defendant could have to forward these documents to her personal email account. *Id.* The fact that Defendant did so twice in the same day further confirms that the acts were intentional and that she wanted to ensure receipt by her personal account. *Id.*

Further preliminary searches have revealed that over the course of the past year, Defendant has emailed large volumes of confidential, inside, and trade secret information to her personal email account. *Id.* at ¶ 8. For instance, on Friday, August 23, 2019, Defendant misappropriated and e-mailed to her personal e-mail account a zip file containing a comprehensive set of all service contracts, leases and other agreements relating to the operations of one of the organization's hospitality assets, a luxury hotel, which she requested and obtained from the operator without the authorization of SFM management. *Id.* These unauthorized e-mails containing SFM business information were sent to Defendant's personal e-mail account with no legitimate SFM business reason. *Id.* Defendant had little or no professional involvement with any of these documents. *Id.* Defendant also sent (again, without authorization) other e-mails to her personal e-mail containing confidential and trade secret information with respect to transactions that had already closed and with respect to which

Defendant had little or no current professional involvement. *Id.*

Strict confidentiality of its methods and procedures concerning the operation of its business is critical to SFM's real estate investment, development and management

In connection with SFM's business, it is critical to maintain the confidentiality of proprietary and trade secret information concerning, *inter alia*, the operations of The Sapir Organization's hotel and luxury condominium properties, the business and economic terms of its leases with tenants at its office and retail properties, the business relationships it maintains, the vendors it uses and the terms of those agreements, the scope of services provided and the technology maintained at its properties, the financial terms of its credit facilities and loan documents, the financial and other terms of its agreements with joint venture and other partners, and its intentions as to acquisitions, dispositions and financings of its assets. *Id.* at ¶ 9. Unauthorized disclosure of such information to a third party would provide critical information to competitive entities that could be used to "roadmap" a competitor in connection with operations, development, acquisitions and business plans, fuel insider trading, and duplicate operational, service and development techniques that The Sapir Organization has spent years, and even decades, establishing. *Id.* Defendant misappropriated and e-mailed to her personal e-mail account such confidential and trade secret information (which SFM will provide to the Court for its confidential review upon request). *Id.*

Key documents misappropriated by Defendant include loan agreements, operating agreements, lease agreements, summary notes of business transactions and vendor agreements, including fees and detailed scope of services, and notes on negotiations with joint venture partners and tenants. *Id.* at ¶ 10. Access to and knowledge of such SFM information, both individually and collectively, would permit competitive entities to compete unfairly with SFM

based upon such access to and knowledge of SFM's non-public business relationship and information concerning its methods and procedures of operation and financial details. *Id.*

For example, on Thursday, June 13, 2019, Defendant misappropriated and e-mailed to her personal e-mail account SFM documents containing a lease summary of all the financial and other material terms of a large tenant at a Sapir Organization office building. *Id.* at ¶ 11. On Wednesday, July 31, 2019, Defendant misappropriated and e-mailed to her personal e-mail account SFM documents containing a lease summary of all the financial and other material terms of another large tenant at a Sapir Organization office building. *Id.* On Thursday, August 1, 2019, Defendant misappropriated and e-mailed to her personal e-mail account several SFM documents consisting of the complete lease with exhibits, all amendments, the lease guarantee and rent, completion and commencement date notice sent by the landlord (*i.e.*, a Sapir Organization company) with respect to another large tenant at the same office building. *Id.*

The information contained in such documents includes highly confidential trade secret information because it could be used by a competitor to lure such tenants away from the Sapir Organization buildings or undercut deals with potential future tenants, give potential future tenants an unfair edge on negotiations, and provide competitors with inside information as to how the buildings are managed and how expenses are recouped, as well as the cost and scope of landlord improvements to the space, landlord's financial allowances to tenants for buildouts, and similar items that could be used to allow competitors to match or undercut terms or duplicate SFM's proprietary formulas for in-house development, construction and management. *Id.* at ¶ 12.

Likewise, on Friday, August 23, 2019, Defendant misappropriated and e-mailed to her personal e-mail account a zip file containing a comprehensive set of service contracts and leases

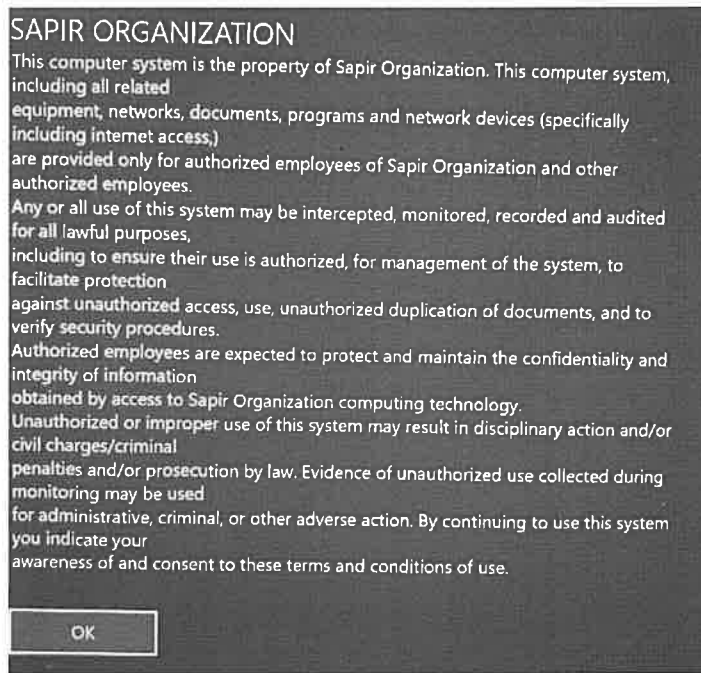
of one of the organization's luxury hotels. *Id.* at ¶ 13. As set forth above, this information provides a collective roadmap of how the organization operates and distinguishes its high-end establishments. *Id.* It is unquestionable that such information is critical to SFM's business operation and constitutes confidential and trade secret information. *Id.*

Similarly, Defendant misappropriated and e-mailed to her personal e-mail account financial data concerning various loans made to The Sapir Organization entities and modifications of same, including highly confidential and trade secret information. *Id.* at ¶ 14. Further demonstrating the illegitimacy of her unauthorized actions, Defendant even misappropriated and e-mailed to her personal e-mail account other SFM confidential and trade secret information concerning deals and transactions which Defendant was not even working on, including negotiations with joint venture partners which had taken place in prior years and with which she had little or no legitimate professional involvement. *Id.*

SFM is vigilant in securing and protecting its confidential and trade secret information

SFM goes to great lengths to protect and secure its proprietary and confidential trade secret information from unauthorized disclosure. SFM's computer network and email files are all password protected. Defendant had 24 hour a day, 7 day a week access to her SFM emails from her cell phone, other mobile device(s) in her possession and control, her desktop and her SFM issued laptop computer (which, upon information and belief, Defendant kept at her residence), including backup access from a web-based platform in case of server issues. *Id.* at ¶ 15. As such, there is/was no reason for her to send materials to her own personal e-mail except for purposes of misappropriating such information and to convert them for her own use or purpose, or for those of a third party. *Id.*

In addition to securing SFM's documents and information with password protection, SFM's employees, including Defendant, are required to read, acknowledge and adhere to the following click through acknowledgement each time they seek to gain access to SFM's computer system:



Id. at ¶ 16. In addition to these frequent (if not daily) reminders of SFM's requirement that Defendant maintain and secure its confidential and trade secret information, SFM's Employee Handbook also expressly states the necessity of protecting and safeguarding the confidentiality of SFM's information. *Id.* at ¶ 17.

Defendant, like all other SFM employees, received a copy of SFM's Employee Handbook at or around the commencement of her employment and periodically thereafter. *Id.* at ¶ 18, Exhibit B (SFM's policy). Indeed, this employee, as part of her duties, worked extensively on updates to the Employee Handbook over the past several years. *Id.* The Employee Handbook contains a policy requiring the protection of SFM's confidential information. *Id.*

As an additional safeguard to SFM's confidential information and trade secrets, Defendant entered into a Confidentiality and Work-For-Hire Agreement with SFM dated March 22, 2016. *Id.* at ¶ 19, Exhibit C. Additionally, Defendant was required to enter into a separate Confidentiality Agreement with SFM in or about March 2018 (the "Confidentiality Agreement"), which superseded the initial March 22, 2016 confidentiality agreement. *Id.* at ¶ 20, Exhibit D (Confidentiality Agreement). Section 2 of the Confidentiality Agreement defines "Confidential Information" as follows:

"[I]nformation relating to the Companies and AS, and their respective affiliates, and each of their respective businesses and properties, which - may include, without limitation, past, present and future investments (existing and potential), financial data and statements, methods and procedures of operation, business plans and ventures (existing and potential), strategies, completed and potential transactions, communications, internal documents and memoranda, e-mails, plans and specifications, drawings, marketing materials, the work product of the Companies' consultants, and other business information, all whether in oral, visual, written, electronic or other tangible or intangible form which is not publically known or available (collectively referred to as the "Confidential Information")".

Id., Exhibit C. Section 3 of the Confidentiality Agreement expressly prohibits Defendant's disclosure of Confidential Information, as defined. *Id.* Likewise, the Confidentiality Agreement also contains an acknowledgement by Defendant that her breach of the Confidentiality Agreement would cause SFM irreparable harm and that the company would be entitled to injunctive relief restraining such disclosure or distribution, in the nature of the relief sought herein. *Id.* at ¶ 24.

Defendant's transmission of SFM's confidential information violated the frequent (if not daily) reminders of SFM's protection of its confidential and trade secret information, which she was required to "click through" in order to gain access to SFM's computer systems, in addition

to violating SFM's policy and the Confidentiality Agreement, and constituted an egregious breach of trust, contract and law. *Id.* at ¶ 25.

SFM reasonably fears that Defendant's knowing, intentional and unauthorized misappropriation of its confidential and trade secret information has caused, or will cause, SFM irreparable harm. *Id.* at ¶ 26. Plainly, Defendant's actions at the expense of SFM were/are for her own personal benefit, or for the benefit of a third-party. *Id.* Defendant has been caught red-handed, and SFM must secure its confidential and trade secret information, obtain its return and prevent its dissemination to third parties. *Id.* SFM simply cannot have its confidential materials reside in a place outside its possession and control. *Id.*

ARGUMENT

SFM IS ENTITLED TO INJUNCTIVE RELIEF

A. Standard of Review

Injunctive relief is appropriate where the party seeking the injunction shows "(a) irreparable harm and (b) either (1) likelihood of success on the merits or (2) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly toward the party requesting the preliminary relief." *Citigroup Glob. Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 35 (2d Cir. 2010) (*quoting Jackson Dairy, Inc. v. H.P. Hood & Sons, Inc.*, 596 F.2d 70, 72 (2d Cir. 1979)). Additionally, injunctions are typically warranted only where the balance of equities tips in the moving party's favor and where an injunction is in the: public interest. *Winter v. Nat. Hus. Def Council, Inc.*, 555 U.S. 7, 20 (2008). For the reasons set forth below, SFM has satisfied these requirements, in addition to those required for relief under the DTSA, and the Court should grant a TRO and Preliminary Injunction to prevent Defendant from continuing to possess (and potentially cause

further damage to SFM as a result of her unauthorized possession of) SFM's trade secrets and proprietary and confidential information.

B. Injunctive Relief is Warranted Under the Defense Trade Secrets Act

Injunctive relief is warranted under the Defense Trade Secret Act (the "DTSA") to:

"[P]revent any actual or threatened misappropriation...on such terms as the court deems reasonable, provided the order does not (1) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence or threatened misappropriation and not merely on the information the person knows; or (2) otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business; [and] if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret."

18 U.S.C. § 1836(3)(A)(I). *See e.g., AUA Private Equity Partners. LLC v. Solo*, No. 17 Civ 803, (S.D.N.Y. November 6, 2017) (granting plaintiff's ex parte motion for temporary restraining order finding that plaintiff will likely succeed on the merits of its DTSA claim); *Mission Capital Advisors LLC v. Romaka*, No. 15 Civ 5878, 2016 WL 11517040 (S.D.N.Y. July 22, 2016) (same); *Henry Schein, Inc. v. Coak*, 191 F.Supp.3d 1072 (N.D. Cal. 2016) (granting a temporary restraining order and preliminary injunction preventing a consultant from accessing, using or sharing confidential data that she stole from her former employer before leaving the company in violation of the DTSA and employment agreement); *Mickey's Linen v. Fischer*, No. 17 C 2154, 2017 WL 3970593 (N.D. Ill. September 8, 2017) (granting injunctive relief finding that defendant would inevitably use or disclose the plaintiff company's trade secrets if was not enjoined from doing so, such that the plaintiff demonstrated a likelihood of success on its trade secrets claims under the DTSA.)

SFM merely seeks to secure the immediate and complete return of its proprietary confidential, trade secret information misappropriated by, and in the possession and control of

Defendant, and to prevent Defendant's dissemination of such information to a competitor, any third party, or other use by Defendant to unfairly compete and harm SFM.

C. SFM Will Suffer irreparable Harm if this Court Does Not Grant Injunctive Relief

SFM will suffer irreparable harm if this Court does not grant injunctive relief. Courts in this Circuit have long acknowledged that “[p]erhaps the single most important prerequisite for the issuance of a preliminary injunction is a demonstration that, if it were not granted the applicant is likely to suffer irreparable harm before a decision on the merits can be granted.” *Payment All. Int'l, Inc. v. Ferreira*, 530 Supp. 2d 477, 480 (S.D.N.Y. 2007) (citation omitted). To satisfy this requirement, SFM must show that it will suffer “an injury that is neither remote nor speculative, but actual and imminent/ and one that cannot be redressed through a monetary award.” *Id.*, quoting *Grand River Enter, Six Nations. Ltd v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007). Appropriately-tailored injunctions can be useful to protect plaintiffs from the effects of misappropriated trade secrets. *See generally, Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 119 (2d Cir. 2009).

In general, the imminent use of a trade-secret constitutes irreparable harm. *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118-19 (2d Cir. 2009) (“A rebuttable presumption of irreparable harm might be warranted in cases where there is a danger that, unless enjoined, a misappropriator of trade secrets will disseminate those secrets to a wider audience or otherwise irreparably impair the value of those secrets”); *North Atlantic Instruments, Inc. v. Haber*, 188 F.3d 38, 49 (2d Cir. 1999); *FMC Corp. v. Taiwan Tainan Giant Indus. Co., Ltd.*, 730 F.2d 61, 63 (2d Cir. 1984) (“[a] trade secret once lost is, of course, lost forever” and, as a result, such a loss “cannot be measured in monetary damages.”); *Estee Lauder Cos. V. Batra*, 430 F. Supp. 2d 158, 174 (S.D.N.Y. 2006) (“Even where a trade secret has not yet been

disclosed, irreparable harm may be found based upon a finding that trade secrets will inevitably be disclosed...).

Here, SFM will be irreparably harmed if Defendant's actions are not immediately curtailed. First, Defendant already acknowledged the potential for irreparable harm when she entered into the Confidentiality Agreement and thereby agreed that injunctive relief is an appropriate remedy:

The Employee, on behalf of himself and the Employee's Representatives, acknowledges and agrees that a breach or threatened breach by the Employee or any of Employee's Representatives of any of the terms, conditions, and provisions of this Agreement will result in irreparable harm to AS and the Companies for which Employer will have no adequate remedy at law and for which damages may be difficult to determine. Accordingly, if any dispute arises concerning the disclosure, distribution or unauthorized use of any Confidential Information in violation of this Agreement or should any term, condition, or provision of this Agreement be breached or should there be a threat of such breach, Employer shall be entitled to seek injunctive relief against the Employee and Employee's Representatives restraining such disclosure, distribution, unauthorized use or violation of the terms, conditions and provisions of this Agreement.

Smith Aff. ¶ 23, Exhibit D. Courts find such acknowledgement to be significant in establishing the potential for irreparable harm so as to justify the imposition of temporary restraints. *See e.g., North Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 49 (2d Cir. 1999) (finding irreparable harm and relying, in part, that defendant "acknowledged in his [e]mployment [a]greement that a breach of the confidentiality clause would cause 'irreparable injury' to [plaintiff]"); *Estee Lauder*, 430 F. Supp. 2d at 174 (same); *Ticor Title Ins. Co v. Cohen*, 173 F. 3d 63, 69 (2d Cir. 1999) (imposing injunction where the Court found that the underlying contract conceded that, in the event of a breach, plaintiff would be entitled to injunctive relief).

Second, injunctive relief is necessary to obtain the return of and prevent the unlawful use of SFM's trade secrets and confidential and proprietary information. Trade secrets can be any "compilation of information which is used in one's business, and which gives [the owner) the

opportunity to obtain an advantage over competitors who do not know or use it.” *Estee Lauder Cos. v. Batra*, 430 F. Supp. 2d 158, 175 (S.D.N.Y. 2006) (summarizing New York law), *quoting* Restatement (First) of Torts § 757, cmt. b (1939). The DTSA definition provides even broader protection to such information, and includes: ...“all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing...” 18 USC § 1839. Such information is considered a “trade secret” if: “(A) the owner thereof has taken reasonable measures to keep such information secret: and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information. 18 USC § 1839(3).²

SFM’s confidential procedures of business operation including, among other things, key business contacts, operating agreements, leases, vendor agreements (including fees and scope of services), technical data, methods and procedures of business operations and financial data (including loan agreements), vendor fees, scope of services and financial data including loan agreement, is the very information upon which SFM’s business is based and certainly constitute trade secrets under either definition, but certainly under the DTSA. Indeed, this information is

² A number of other factors also bear on whether information is truly a trade secret, including “(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.” *Estee Lauder Cos. v. Batra* at 175.

the product of a vast amount of SFM's time, effort and resources and would be highly useful to a competitor. Such trade secret information could be used by a competitor to lure tenants away from the Sapir Organization's buildings or undercut deals with potential future tenants, give potential future tenants an unfair edge on negotiations, and provide competitors with inside information as to how such buildings are managed and how expenses are recouped, as well as the cost and scope of landlord improvements to the space, landlord's financial allowances to tenants for buildouts, and similar items that could be used to allow competitors to match or undercut terms or duplicate SFM's proprietary formulas for in-house development, construction and management.

SFM took pains to maintain the confidentiality of its trade secrets, including ensuring all computer files and emails are password protected, requiring acknowledgement of the confidentiality of SFM's data each and every time an individual accessed SFM's computer system, a confidentiality policy in the Employee Handbook, along with a broad confidentiality provision in Defendant's Confidentiality Agreement. *See* Smith Aff. ¶¶ 14 – 22, Exhibits B-D. This confidential, proprietary and trade secret information is hugely valuable to SFM, as it would be to SFM's competitors because such data could be used as a "roadmap" for acquisitions, development and providing services that SFM has spent years, and even decades establishing.

Moreover, absent restraint, SFM's damages associated with losing its trade secrets would alone be incalculable, Defendant, armed with SFM's confidential proprietary and trade secret information, is in prime position to cause further irreparable harm to SFM's business and reputation. SFM could not possibly track what business opportunities have been, and will be, lost and money damages thus would prove an inadequate remedy.

D. SFM is Likely to Succeed on the Merits of Its Underlying Claim

To establish a likelihood of success on the merits, a plaintiff “need not show that success is an absolute certainty. He need only make a showing that the probability of his prevailing is better than fifty percent.” *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495, 509 (S.D.N.Y. 2017) (citation omitted). SFM plainly meets its burden in this action.

1. The DTSA Claim

The DTSA amends the existing federal Economic Espionage Act (the “EEA”) (18 U.S.C. § 1831, *et. seq.*) and creates a federal cause of action for the misappropriation of trade secrets used in interstate commerce. The DTSA requires plaintiff to establish “an unconsented disclosure or use of a trade secret by one who (i) used improper means to acquire the secret, or (ii) at the time of disclosure, knew or had reason to know that the trade secret was acquired through improper means, under circumstances giving rise to a duty to maintain the secrecy of the trade secret, or derived from or through a person who owed such a duty.” *Free Country Ltd v. Drennen*, 235 F.Supp.3d 559, 565 (S.D.N.Y. 2016); *see also* 18 U.S.C. § 1839(5). The DTSA’s definition of “improper means” includes “misrepresentation, [and] breach or inducement of a breach of a duty to maintain secrecy,” but expressly excludes “reverse engineering” and “independent derivation.” 18 U.S.C. § 1839(6)(A)-(B).

As set forth above, the material misappropriated by Defendant by her calculated and systematic actions, fall squarely within the scope of the DTSA. *See AUA Private Equity Partners, LLC v. Solo*, No. 17-8035, 2018 WL 2684339, *7 (S.D.N.Y. April 5, 2018) (holding that complaint plausibly alleges violation of the DTSA as defendant was alleged to have uploaded plaintiffs trade secrets from her work laptop to her personal cloud-based storage without plaintiff’s permission and in direct violation of the confidentiality agreement that she

signed); *RKI, Inc., d/b/o Roll-Kraft v. Grimes*. 177 F.Supp.2d 859, 875-77 (N.D. Ill. 2001) (finding sufficient evidence of acquisition of theft when employee downloaded or copied trade secrets from work computer to home computer). First, Defendant misappropriated the protected material *after* entering a Confidentiality Agreement in which she (a) acknowledged that such documents and information are trade secrets, and (b) contracted and covenanted (thereby generating a duty resulting from her employment and by contract), she would not divulge or download SFM's trade secrets and confidential and proprietary information. Second, the information Defendant misappropriated from SFM is not readily ascertainable. No one can reverse engineer, or learn by research alone, how SFM sets its business model apart from competitors, the terms of its operating and lease agreements, who are SFM's key vendors, the fees and scope of services they provide, or the financial terms of its loan documents. Armed with this information, a competitor could create a complete and comprehensive threat to SFM's business far faster than one that has not engaged in unlawful competition arising out of the theft of SFM's trade secrets. Third, SFM vigilantly safeguards its data by requiring password protection on all computer and e-mail files, frequently (if not daily) acknowledgements of SFM's interest in safeguarding its data, employment policies and requiring the execution of a confidentiality agreement as a condition of employment.

2. New York's Trade Secret Law

SFM is also likely to succeed under the New York Trade Secret law, for which it will demonstrate: (1) that Defendant possessed a trade secret; and (2) that Defendant used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means. For the reasons set forth above in support of its DTSA claim, SFM also satisfies the foregoing elements. *See Eastern Bus. Sys., Inc. v. Specialty Bus. Solutions*, 292

A.D.2d 336, 337-38, (2d Dept. 2002) (client and potential client names, addresses, contact names compiled through considerable effort over several years and not available to the public are trade secrets warranting protection); *Ashland Mgmt. Inc. v. Janitn.* 82 N.Y.2d 395, 407 (1993) (“[C]onfidential proprietary data relating to pricing, costs, systems, and methods are protected by trade secret law.”); *N. All. Instruments, Inc. v. Haber*, 188 F.3d 38, 44 (2d Cir. 1999) (“Numerous cases applying New York law have held that where ... it would be difficult to duplicate a customer list because it reflected individual customer preferences, trade secrets protection should apply.”)

3. Breach of Contract

Given the substantial evidence described here, there is no doubt SFM will also succeed on its breach of contract claim against Defendant. To state a claim under New York law for breach of contract, a plaintiff must plead: (1) a contract; (2) performance of the contract by one party; (3) breach by the other party; and (4) damages. *First Inv'rs Corp. v. Liberty Mut. Ins. Co.*, 152 F.3d 162, 168 (2d Cir. 1998). Here, Defendant entered a Confidentiality Agreement in or about March 2018. SFM performed its obligations under the Confidentiality Agreement and Defendant breached her obligations thereto by, among other things, misappropriating SFM's trade secrets and confidential information, which breach resulted in damages to SFM as discussed herein.

4. Breach of Duty of Loyalty

New York law with respect to disloyal or faithless performance of employment duties is grounded in the law of agency and has developed for well over a century. *Phansalkar v. Andersen Weinroth & Co. L.P.*, 344 F.3d 184, 200 (2d Cir. 2003). An agent is obligated under New York law to be loyal to her employer and is “prohibited from acting in any manner

inconsistent with his agency or trust and is at all times bound to exercise the utmost good faith and loyalty in the performance of his duties.” *Id.* This duty is not dependent upon an express contractual relationship but exists even where the employment relationship is at-will. *Id.*; accord *Design Strategies, Inc. v. Davis*, 384 F.Supp.2d 649, 659-60 (S.D.N.Y. 2005); see also *W. Elec. Co. v. Brenner*, 41 N.Y.2d 291, 295, 392 N.Y.S.2d 409, 360 N.E.2d 1091 (1977) (“The employer-employee relationship is one of contract, express or implied, and, in considering the obligations of one to the other, the relevant law is that of master-servant and principal-agent.”) (citations omitted).

For the reasons described above, it is unquestionable that Defendant knowingly and intentionally breached her duty of loyalty by maliciously converting SFM’s trade secrets and confidential information to, upon information and belief, advance her own personal interest, or that of a third-party, at the expense of SFM. Accordingly, SFM will also be successful on its claim for Defendant’s breach of her duty of loyalty under New York law.

E. The Balance of the Equities, the Evidence, and the Public Interest Tip Strongly in Favor of SFM

The balance of equities and the public interest favors entering an order that would mandate the immediate return of SFM’s misappropriated material. First, Defendant has no legitimate interest in, or claim to, SFM’s trade secrets and proprietary information and the DTSA expressly precludes the acquisition of trade secrets by improper means -- which is exactly what Defendant has done. Moreover, given the direct evidence of misappropriation, there is no question that Plaintiff will likely succeed on the merits. Second, she has breached her Confidentiality Agreement and duty of loyalty by removing them from SFM. Third, dissemination of the misappropriated trade secrets will have a significant detrimental impact on SFM and will irreparably damage its goodwill in the market place should its methods and

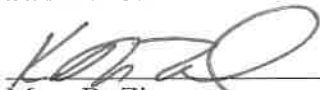
procedures of operation and financial data become public knowledge -- a result that will not be remediated by money damages. *See Juergensen Def. Corp, v. Carleton Techs. Inc.*, No. 08-CV-959A, 2010 WL 2671339 (W.D.N.Y. June 21, 2010) (finding that balance of equities and public interest favored injunction where disclosure of trade secrets would ruin plaintiffs). In contrast, an injunction would have no significant impact on Defendant because it would simply require her to return information belonging to SFM to which Defendant should not be in possession of in the first place.

CONCLUSION

For all of the foregoing reasons, SFM respectfully requests that this Court issue a temporary restraining order, and a preliminary injunction and such other and further relief as this Court deems just and proper against Defendant. SFM reserves the right to petition the Court for a seizure order should Defendant fail to abide by the Orders of this Court pertaining to locating, isolating, and returning to SFM its misappropriated material.

Dated: New York, New York
January 9, 2020

FREEBORN & PETERS, LLP



Marc B. Zimmerman
Kathryn T. Lundy
230 Park Avenue, Suite 630
New York, New York 10169
(212) 218-8760
Attorneys for Plaintiff